Release Notes for Cisco Secure Email Encryption Plug-in 1.2.1

Published: July 07, 2020
Last Updated: November 28, 2022

Contents

Cisco Systems, Inc.
www.cisco.com

What's New in this Release

What's New in Release 1.2.1-212

The Cisco Secure Email Encryption Plug-in release 1.2.1-212 consists of a bug fix. For more information, see List of Fixed Issues, page 5.

What's New in Release 1.2.1-204

Feature	Description
Option for Selecting Storage Preference	You can configure the preferred storage to save a copy of the encrypted envelope when this feature is enabled. The following storage options are available: • Cisco Storage • Microsoft OneDrive Storage For more information, see Cisco Secure Email Encryption Service Account Administrator Guide.

Note The external storage feature is available in English language only. Other languages are not supported for this feature in this release.

Supported Configurations

The following configurations are supported for the Cisco Secure Email Encryption Plug-in 1.2.1.

Cisco Secure Email Encryption Plug-in 1.2.1	Outlook 2016	Outlook 2019	Office 365
Microsoft Windows Enterprise	compatible	certified	certified

Note When you upgrade to Office 365, Cisco Secure Email Encryption Plug-in may be disabled in your Outlook. In that case, you must enable it manually.

Note Support for Microsoft Windows 7 and 8.1 versions was available till the Cisco Secure Email Encryption Plug-in version 1.2.1-151. Now, there is only support for Microsoft Windows Enterprise.

Important Note About Installing or Updating Java

We recommend that you do not update Java (Oracle or Open JRE) manually. If you still want to update Java, then you must take care of the following points while upgrading Open JRE to Eclipse Adoptium:

- Choose *Entire feature will be installed on local hard drive* for **Set JAVA_HOME variable** and **JavaSoft Registry keys** during the installation.
- If you are using command line to update Open JRE, use the following command:

```
msiexec /i OpenJDK11U-jre_x64_windows_hotspot_11.0.14_9.msi
INSTALLLEVEL=3 /quiet
```

If you have already installed Eclipse Temurin JRE, you must uninstall it and then install the Cisco Secure Email Encryption Plugin 1.2.1-204 which contains the Eclipse Temurin JRE bundled with it.

Upgrading to Cisco Secure Email Encryption Plug-in 1.2.1

- Upgrade Paths, page 3
- Upgrading the Cisco Secure Email Encryption Plug-in, page 3
- Upgrading from Cisco Secure Email Security Plug-in to Cisco Secure Email Encryption Plug-in, page 4

Upgrade Paths

You can upgrade to Cisco Secure Email Encryption Plug-in 1.2.1-212 from the following component versions:

- Cisco Secure Email Security Plug-in 7.6.2.037
- Cisco Secure Email Encryption Plug-in 1.2.1-204

Note After you update the Cisco Secure Email Security Plug-in 7.6.2.037, the Cisco Secure Email Security Plug-in will be removed and the Cisco Secure Email Encryption Plug-in will be available instead.

Upgrading the Cisco Secure Email Encryption Plug-in

Note The Secure Email Security Plug-in does not display the expiry date on the secure message (below the **Read Message** button, if you have enabled Easy Open). So, you must upgrade the Secure Email Security Plug-in to Secure Email Encryption Plug-in.

Note Before upgrading the Cisco Secure Email Encryption Plug-in, see Important Note About Installing or Updating Java, page 3.

To upgrade the Cisco Secure Email Encryption Plug-in:

Step 1 Download the Email Encryption Plug-in installer from the Cisco Software Download Center.

Step 2 Double-click the *Cisco Email Encryption Plug-in.exe* file.

Step 3 In the **Cisco Email Encryption Plug-in Setup** window, select a language, and then click **OK**.

Step 4 In the message that appears, click **OK** to start an upgrade. The previous version of the Cisco Secure Email Encryption Plug-in will be removed.

Step 5 Click **Next** to continue upgrading the Cisco Secure Email Encryption Plug-in.

Step 6 Click **Install** to start installing the latest version.

Step 7 Wait until the Setup Wizard installs the Cisco Secure Email Encryption Plug-in, and click **Finish**.

Note If you cannot upgrade the Cisco Secure Email Encryption Plug-in, uninstall all previous versions of the plug-in and then perform a fresh install.

Upgrading from Cisco Secure Email Security Plug-in to Cisco Secure Email Encryption Plug-in

Note Before upgrading from Cisco Secure Email Security Plug-in to Cisco Secure Email Encryption Plug-in, see Important Note About Installing or Updating Java, page 3.

To upgrade from the Cisco Secure Email Security Plug-in to the Cisco Secure Email Encryption Plug-in:

Step 1 Download the Email Encryption Plug-in installer from the Cisco Software Download Center.

Step 2 Double-click the *Cisco Email Encryption Plug-in.exe* file.

Step 3 In the **Cisco Email Encryption Plug-in Setup** window, select a language, and then click **OK**.

Step 4 In the message that appears, click **OK** to start an upgrade. The Cisco Secure Email Security Plug-in will be removed and the Cisco Secure Email Encryption Plug-in will be installed.

Step 5 Click **Next** to continue upgrading the Cisco Secure Email Encryption Plug-in.

Step 6 Click **Install** to start installing the latest version.

Step 7 Wait until the Setup Wizard installs the Cisco Secure Email Encryption Plug-in, and click **Finish**.

Note The Cisco Secure Email Security Plug-in will be removed from the Outlook toolbar, and the Cisco Secure Email Encryption Plug-in will be available instead.

Installing Cisco Secure Email Encryption Plug-in 1.2.1

- Installing the Cisco Secure Email Encryption Plug-in, page 5
- Performing Mass Installation of Cisco Secure Email Encryption Plug-in, page 5

Installing the Cisco Secure Email Encryption Plug-in

Note Do not use or install the Cisco Secure Email Encryption Plug-in 1.2.1 with the Cisco Secure Email Security Plug-in 7.6.0 or later. If you need the reporting functionality, install both the Cisco Secure Email Encryption Plug-in 1.x and the Cisco Secure Email Reporting Plug-in 1.x.

Note Before installing Cisco Secure Email Encryption Plug-in, see Important Note About Installing or Updating Java, page 3.

To install the Cisco Secure Email Encryption Plug-in:

Step 1 Download the Email Encryption Plug-in installer from the Cisco Software Download Center.

Step 2 Double-click the *Cisco Email Encryption Plug-in.exe* file.

Step 3 In the **Cisco Email Encryption Plug-in Setup** window, select a language, and then click **OK**.

Step 4 Click **Next** to start the installation program.

Step 5 Click **Install**.

Step 6 Wait until the Setup Wizard installs the Cisco Secure Email Encryption Plug-in, and click **Finish**.

Performing Mass Installation of Cisco Secure Email Encryption Plug-in

See *Cisco Secure Email Encryption Plug-in 1.2.1 Administrator Guide* for instructions on how to perform mass installation of Cisco Secure Email Encryption Plug-in.

List of Fixed Issues

- CSCwc43698 -Microsoft Outlook crashes when encrypting emails from Encryption Plug-in.

Related Documentation

For more information about the Cisco Secure Email Encryption Plug-in, see:

- *Cisco Secure Email Encryption Plug-in 1.2.1 Administrator Guide*. This guide provides instructions for installing and configuring the Cisco Secure Email Encryption Plug-in, and it may help you to understand how to configure your encryption settings to work with the plug-in settings you configure.
- *Cisco Secure Email Encryption Plug-in 1.0 Open Source Documentation.* This document contains licenses and notices for open source software used in this product.

Service and Support

You can request support by phone, email, or online 24 hours a day, 7 days a week. Cisco Customer Support service level agreement details are available on the Support Portal. You can contact Cisco Customer Support using one of the following methods:

- Cisco Support Portal: https://www.cisco.com/support
- Phone support: Contact Cisco Technical Assistance Center (TAC) within U.S. /Canada at 800-553-2447 and at Worldwide Phone Numbers.
- Email: tac@cisco.com

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

To have a list of all new and revised Cisco technical documentation delivered directly to your desktop using a reader application, subscribe to *What's New in Cisco Product Documentation* as an RSS feed by clicking the RSS icon on the What's New page. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.